Reversible medical image watermarking for tamper detection and recovery

CONFERENCE PAPER · JULY 2010

DOI: 10.1109/ICCSIT.2010.5564078

CITATIONS
10

READS
70

2 AUTHORS:

Siau-Chuin Liew
Universiti Malaysia Pahang
18 PUBLICATIONS **26** CITATIONS
SEE PROFILE

Jasni Mohamad Zain
Universiti Malaysia Pahang
69 PUBLICATIONS **293** CITATIONS
SEE PROFILE

Reversible Medical Image Watermarking For Tamper Detection And Recovery

Siau-Chuin Liew
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
eliewsc@gmail.com

Jasni Mohamad Zain
Faculty of Computer Systems and Software Engineering
Universiti Malaysia Pahang
Kuantan, Malaysia
jasni@ump.edu.my

***Abstract*— This research paper discussed the usage of watermarking in medical images to ensure the authenticity and integrity of the image and reviewed some watermarking schemes that had been developed. A design of a reversible tamper detection and recovery watermarking scheme was then proposed. The watermarking scheme uses a 640x480x8 bits ultrasound grayscale image as a sample. The concept of ROI (Region Of Interest) and RONI (Region Of Non Interest) were applied. Watermark embedded can be used to detect tampering and recovery of the image can be done. The watermark is also reversible.**

Keywords-component; watermark; tamper detection; recovery; reversible; medical image

I. INTRODUCTION

In modern health care facilities, systems such as HIS (Hospital Information System) and PACS (Picture Archiving and Communications System) form the information technology infrastructure for a hospital. Advancements in medical information system is changing the way patient records are stored, accessed and distributed. The integrity of the records such as medical images needs to be protected from unauthorized modification or destruction of information on the medical images. Current security measures used to protect the integrity of the patient records are such as VPN (Virtual Private Network), data encryption and data embedding [1].

Data encryption is being used on the Internet to protect sensitive data during transmission. It is also being used to protect medical images in the form of digital signature. The problem with digital signature is that it needs to be transmitted together with the image in a separate file or in the image header. There is also a risk of losing the signature during transmission. The signature will also be lost if the image file is converted to another format that does not allow headers. Data embedding is where related information such as digital signature can be inserted into the medical images as a watermark. Currently, there is no standard of implementation for digital watermarking. Watermark provides three objectives in medical images [2]:

- data hiding, for embedding information to make the image useful or easier to use;
- integrity control, to verify that the image has not been modified without authorization;
- authenticity, that is to verify that the image is really what the user supposes it is.

In practice diagnoses has been performed on medical images before being directed to the long-term storage, thus the significant part of the image is already been determined by doctors involved in the diagnosing process [3]. The significant part is called ROI (Region Of Interest). Since information in medical images is not to be modified in any way, the watermark is usually being embedded in the RONI (Region Of Non Interest) as this region does not contribute in the process of diagnosis. Another option is to allow the watermark to be reversible [2]. The usage of ROI in watermarking in medical images had been used by Lim et al [4] and Fotopoulus et al [5] where ROI and RONI were defined before the process of watermark embedding. Reversible watermarking is where embedded watermark is removed and the original pixel value is restored. Research by Coatrieux et al [6] produced a watermarking scheme where information describing the image is embedded into medical images and can be reversed later on.

The ability of to detect tampering of a watermarked image is crucial for authentication. Once tampering is detected, tampered section can be recovered. Research by Wu et al [7] and Jasni and Abdul [9] divides medical image into blocks and each block is embedded with the authentication message and recovery information of other blocks. Tampered blocks can then be restored using this information.

In this paper, we propose a reversible tamper detection and recovery for medical image. This design will be using ROI, RONI and blocks to divide the medical image. Authentication bit, parity bit and pixels average intensity will be used to detect tampering and recovery.

In the next section, watermarking in medical images and related work is introduced. The proposed scheme is described in section three. The results of the watermarking experiment are presented in section four. Finally, the conclusion is in section four

978-1-4244-5540-9/10/$26.00 ©2010 IEEE

II. WATERMARKING IN MEDICAL IMAGES

Before proceeding to the design of the watermarking scheme, the foundation of digital watermarking, types of domain and performance measurement methods is discussed in this section. Fundamentally, watermarking system is shown as in Fig. 1.

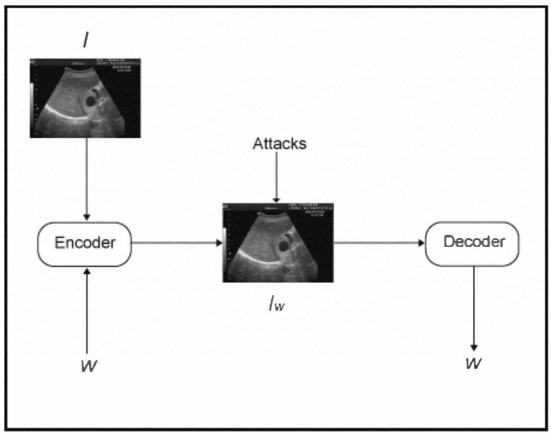

Figure 1. Watermark is embedded into an image using an encoder and extracted using a decoder.

The encoder, E embeds the watermark, W inside original image I by using embedding function, E as shown in equation (1).

$$E(I, W) = I_W \tag{1}$$

The output from this process is I_W, the watermarked image. The decoder, D will detect or extract the watermark, W from the original image as in equation (2).

$$D(I, I_W) = W \tag{2}$$

A. Types of domain

Watermarking techniques can be classified according to how the watermark is embedded namely within the spatial domain or in transform domains.

1) Spatial domain

One of the most direct and simple technique is to embed the watermark code into the LSBs (Least Significant Bits) of the image. Since a change in LSB corresponds a change in 1 unit of image gray value, its modification is not perceivable by human eyes. This technique is not as robust as transform domain techniques and rarely survives various attacks.

2) Transform domain

Most of the transform domain techniques embed watermark information into the transform coefficients of the cover image. DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform) and DFT (Discrete Fourier Transform) are the three popular methods in this category. These methods require a longer computation time but they are compatible with image compression and more robust against geometric transformation such as rotation, scaling, translation and cropping.

B. Performance measures

The performance of the watermarking is crucial to ensure the fidelity and quality of the watermarked images. Watermarking performance can be measured in terms of perceptibility. Below are two methods that can be used.

1) MSE(Mean Square Error)

MSE is one of the simplest functions to measure the perceptual distance between watermarked and unwatermarked images. This is defined as:

$$MSE = \frac{1}{n}\sum_{i}^{n}\left(I_i' - I_i\right)^2, \tag{3}$$

which is average term by term difference between the original image, I, and the watermarked image, I'.

2) PSNR(Peak Signal to Noise Ratio)

It is used to measure the similarity between images before or after watermarking. This is defined as:

$$PSNR(dB) = 10\log_{10}\frac{\max I^2}{MSE}, \tag{4}$$

where max I is the peak value of the original image.

C. Watermarking schemes

There are very few tamper detection and recovery watermarking scheme for medical image. An example is the scheme developed by Wu et al [7]. The scheme divides an image into blocks and each block is embedded with the authentication message and the recovery information of other blocks. Hash value is calculated for each block and JPEG bits from another block is retrieve before being embedded as watermark into another block. The detection of the tampering is done by comparing the hash value embedded together with the watermark and the hash value extracted from the image. If tampering is detected, recovery information is extracted from the corresponding block. The schemes can recover the whole image or only the ROI.

Reversible watermarking had been proposed by Coatrieux et al [6]. Knowledge digest that gives a synthetic medical description of the medical image content is used for retrieving similar images with either same findings or different diagnoses. The knowledge digest is embedded as a reversible watermarking.

Jasni et al [8] developed a reversible watermarking where hash function is used to protect the ROI. Hash value of the whole image is embedded in the RONI as the watermark. The beauty of ultrasound images and all other medical images is that the LSBs for all pixels in the RONI are zeroes [8]. The watermark is reversed by simply setting the LSBs of RONI back to zero.

III. METHODOLOGY

The design of this watermarking scheme is based on the scheme proposed in [9] in terms of watermark embedding, tamper detection and recovery. Further developments were made in image preparation, embedding and storing of original bits to allow this watermarking scheme to be reversible.

A. Image preparation

Image preparation is the key for this scheme to be reversible. We had taken a different approach by dividing a 640x480 pixels ultrasound image into ROI and RONI as shown in Fig. 2.

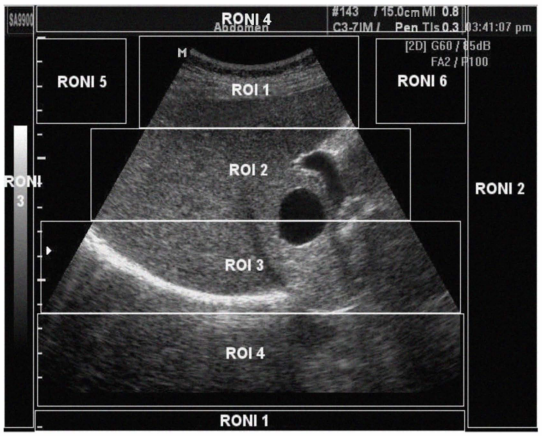

Figure 2. Ultrasound image divided into ROI and RONI

Scheme developed by Fotopoulos et al [5] and Jasni et al [8] uses a rectangle to define the ROI of the medical image. In our scheme, we used four rectangles to form a pyramid shape for the ROI. This method allow the ROI to be more accurately defined due to the characteristic of the ultrasound image and results in more space being used for defining the RONI. There are six rectangles in the RONI .The ROI will be divided into blocks of 8x8 pixels and RONI into blocks 6x6 pixels. The number of blocks in the ROI must not exceed the number of blocks in the RONI to ensure that the original LSBs that will be removed from the ROI for watermark embedding can be stored in the RONI without storage issue.

One-to-one mapping which is similar mapping sequence proposed by [9] will be used as shown in (5) below:

$$\vec{B} = \left[(k \times B \bmod N_b\right] + 1 \qquad (5)$$

where $B, \vec{B}, k \in [1, N_b]$,k is a prime number, and N_b is the total number of blocks in the ROI.

In our scheme, we assign a unique integer $B \in \{1,2,3,\ldots, N_b\}$ to each block in the ROI. Number of blocks in the RONI is equal to the total number of blocks in the ROI. The maximum prime number $k \in [1, N_b]$ is picked. Equation (5) is applied to each block number B where $\vec{B}$, the number of its mapping blocks in obtained. All pairs of B and $\vec{B}$ will form the block mapping sequence for ROI. Blocks in the RONI are also assigned with a unique integer. Each block in RONI corresponds with the blocks in ROI. In our scheme, for example as shown in Fig.3, block x1 is mapped to block y1 in ROI by using equation (5). Block x1 in the ROI with unique integer "5" for example, is mapped with block x2 in the RONI with the same integer. The same algorithm is applied in mapping block y1 and block y2.

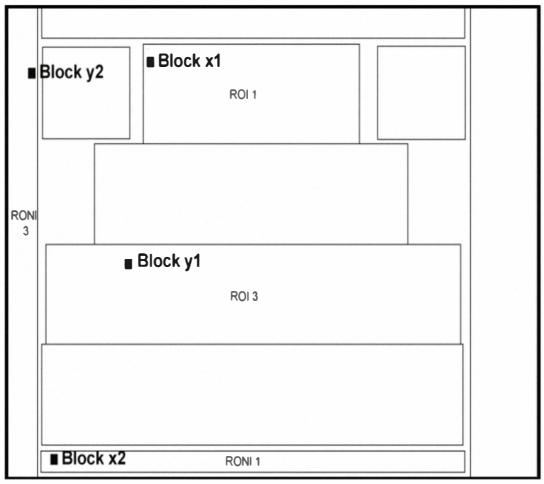

Figure 3. Mapping sequence between blocks in ROI and RONI

B. Embedding

1) Watermark

The watermark embedding algorithm is based on the work in [9] where each block of 8x8 pixels in the ROI is divided into four sub-blocks of 4x4 pixels. The watermark in each sub-block is a block of 3x3 pixels where it contains two-bit authentication watermark and a seven-bit recovery watermark for the corresponding sub-block within block x1 mapped to block y1.

We have taken a different approach in the removal of LSBs significant bits. Only the LSBs for pixels which will be used for watermarking will be removed as compare to removal of LSBs for each pixel within the block as proposed by Jasni and Abdul [9]. Figure 4 shows that only the block of 3x3 pixels in each sub-block where the LSBs will be set to zero. This will minimize processing time needed and ensure storage availability in the RONI for the LSBs which were removed from the ROI.

Average intensity for each block and its sub-blocks will be computed. Authentication bit and parity bit is generated for each sub-block. From the mapping sequence generated in the image preparation step, block y1 recovery information will be stored in block x1. The average intensity of sub-blocks y1s within block y1, denoted as avg_y1s will be computed as the recovery intensity. The authentication bit, parity bit and the recovery intensity form the watermark where they will be embedded in the corresponding LSBs in the sub-blocks of x1.

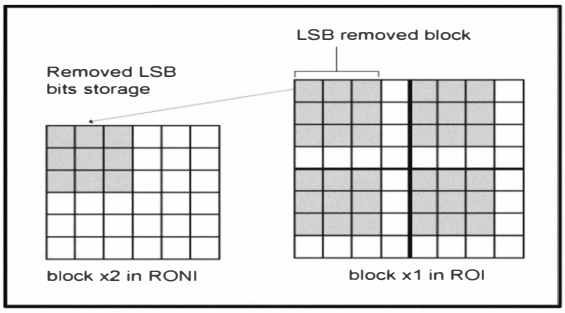

Figure 4. Block x1 and block x2

2) Removed LSBs

We proposed that the LSBs that were removed from the watermark embedding process to be stored in the RONI for the usage of restoring of the ROI to its original bits later. By using the example in Fig 3. and Fig 4., LSBs of block x1 that were removed will be stored in LSBs of block x2 in the RONI. Each of the 3x3 pixel block in the RONI will store the LSBs that were removed from the corresponding sub-block in the ROI by matching the block number that were assigned in the preparation step.

C. Tamper detection and recovery

The ROI of the image is divided blocks of 8x8 pixels and the LSBs in the sub-block of 4x4 pixels will be removed, as in the watermarking embedding process.

As proposed by Jasni and Abdul [9], the average intensity of the block will be computed. For each sub-block of 4x4 pixels, authentication bit and parity bit will be extracted. The LSBs in the sub-block will be set to zero and average intensity for each sub-block will be computed. Authentication bit and parity bit generated from the average intensity of block and sub-block will be compared to know whether the block is tampered. Tampered blocks will be recovered by locating its corresponding blocks by using the mapping sequence used in image preparation. By referring to Fig 3., with the assumption that block y1 had been tampered and its recovery bits were stored in block x1,the average intensity of each sub-block of block y1 stored in sub- blocks of block x1 will be obtained. Block y1 will be replaced with the recovered average intensity bits.

D. Reversible watermark

As an addition function to the scheme by Jasni and Abdul [9], here we proposed that the embedded watermark can be reversed by restoring removed LSBs during the watermark embedding process. Removed LSBs of block x1 were stored in block x2 in the RONI as shown in Fig.3. The LSBs of each sub-block x1 will be replaced with its original bits that were stored in the 6x6 pixels of block x2 as shown in Fig.4. The process is applied to every block in the ROI. The LSBs of each pixel in RONI will be reset back to its original value which is zero.

CONCLUSION

This paper proposed a design of a reversible tamper detection and recovery watermarking for medical images. A reversible watermarking scheme is crucial to allow the original pixel values to be restored. Further testing is required to know the perceptibility of the watermarked image. An area of possible further development is the security of the embedded original pixel value in the RONI. Hash function could be used to verify the authenticity and integrity of the original pixel values.

ACKNOWLEDGEMENT

We would like to thank Research and Innovation Centre of Universiti Malaysia Pahang for the financial support provided for the research work.

REFERENCES

[1] Cao,F.,Huang,H.K.,Zhou,X.Q., "Medical image security in a HIPAA mandated PACS environment",*Computerized Medical Imaging and Graphics*,2003,vol 27,pp.185-196, doi:10.1016/S0895-6111(02) 00073-3

[2] Coatrieux, G., Main, H., Sankur, B., Rolland, Y., Collorec, R., "Relevance of watermarking in medical imaging", in *Proc. of IEEE-EMBS Information Technology Applications in Biomedicine*,IEEE, Nov 2000, pp. 250-255, doi:10.1109/ITAB.2000.892396.

[3] Wakatani,A., "Digital Watermarking for ROI Medical Images by Using Compressed Signature Image," in *Proc. 35th Annual Hawaii International Conference on System Sciences (HICSS-35'02)*,IEEE Conference Publishing,Jan 2002, pp. 2043-2048.

[4] Lim,Sung Jin,Moon, Hae Min,Chae, Seung-Hoon,Pan, Sung Bum, Yongwha Chung, Min Hyuk Chang, "Dual watermarking method for integrity of medical images", in *Proc. of Second International Conference on Future Generation Communication and Networking*, ,IEEE Conference Publishing,Dec 2008, vol.2, pp.70-73, doi: 10.1109/FGCN.2008.

[5] Fotopoulos,V., Stavrinou ,M.L, Skodras,A.N., "Medical image authentication and self-correction through an adaptive reversible watermarking technique " in *Proc. of the 8th IEEE International Conference on BioInformatics and BioEngineering*,IEEE Conference Publishing, Oct 2008, pp.1-5,doi: 10.1109/BIBE.2008.4696803.

[6] Coatrieux, G, Le Guillou, C., Cauvin, J.-M., Roux, C., "Reversible watermarking for knowledge digest embedding and reliability control in medical images", *IEEE Transactions on Information Technology in Biomedicine,* vol 13, issue 2, Mac 2009,pp.158 – 165,doi: 10.1109/TITB.2008.2007199.

[7] Wu ,Jeffery H. K, Chang ,Ruey-Feng, Chen,Chii-Jen, Wang ,Ching-Lin, Kuo ,Ta-Hsun, Moon,Woo Kyung ,Che ,Dar-Ren, "Tamper detection and recovery for medical images using near-lossless information hiding technique", *Journal of Digital Imaging*, Mac 2008 , vol 21,No 1,pp. 59-76,doi: 10.1007/s10278-007-9011-1.

[8] Jasni M. Zain, L.P Balwin,M.Clarke,"Reversible watermarking for authentication of DICOM images", in *Proc. 26th Annual International Conference of the IEEE EMBS*, IEEE Conference Publishing , Sep 2004,pp. 3237 - 3240 ,ISBN: 0-7803-8439-3.

[9] Jasni M. Zain, Abdul R.M. Fauzi, "Medical Image Watermarking with Tamper Detection and Recovery", in *Proc. 28th Annual International Conference of the IEEE EMBS*, IEEE Conference Publishing,Sept. 2006,pp. 3270-3273,doi: 10.1109/IEMBS.2006.260767.